Byram Hills School District, Armonk, NY

TECHNOLOGY and NETWORK ACCEPTABLE USE and PERSONAL PRIVACY 4526

The Board of Education encourages the use of technology in District classrooms for the purpose of advancing and promoting learning and teaching, and also encourages users to develop appropriate skills and use judgment when utilizing such resources. District or personal electronic devices connected to the network may only be used in a manner consistent with this policy, the Code of Conduct, and all other District policies. These policies apply to all users who gain access to District technology or the Internet while on school grounds or at school events. This also includes any remote access which users may gain from off-site, but which involves the use of District sites, servers, intranet facilities, e-mail accounts or software.

The District recognizes that with technology access comes the availability of material which is unrelated to scholarship, and which in many instances is inappropriate for places of learning. Although the District, in cooperation with the Board of Cooperative Educational Services (BOCES), has taken precautions to restrict access to questionable materials, students and parents need to know that it is impossible to control all materials, so responsibility rests with the user. Users who violate this policy, or who access, alter, delete, damage or destroy any computer system, wireless access, computer program, or data without permission will be subject to disciplinary action by the District and may in appropriate cases be referred for criminal prosecution.

Use of the systems network and technology, specifically including but not limited to District e-mail, can and will be monitored by the District, at any time, to ensure that the system is being used properly. There is no expectation of privacy with respect to use of District e-mail or any materials stored on or communicated through District facilities.

The District makes no warranties of any kind, whether express or implied, for the service it is providing. It is not responsible for any damages, including loss of data resulting from delays, non-deliveries, miss-deliveries, or service interruptions, whether caused by the District or third party negligence, or by a user's errors or omissions. Information obtained from the Internet is used at the user's own risk, and the District specifically disclaims any responsibility for the accuracy or quality of information obtained via access provided by or through the District.

The director of technology will oversee the use of District technology resources and will prepare programs for the training and development of District users in technology skills and applications. All users of the District's technology and the Internet must annually agree to comply with the guidelines for usage in this policy, as per District procedure.

Permitted and Prohibited Uses of District Technology Resources

1. Technology, network and the Internet are to be used primarily for purposes directly related to work, teaching or scholarship. Incidental personal use shall not be deemed a waiver of the District's right to prohibit all such use, either on an individual or on a general basis.

2. Each teacher has reasonable discretion to allow and regulate student use of District and personal electronic devices in the classroom for the purpose of specific class-related projects, consistent with all District policies.

3. The network may not be used:

    a. to download, copy, store or install any software, unless approved in advance, and on a specific case-by-case basis, by the director of technology;

    b. for any personal commercial enterprise;

    c. to sell products or services, or for advertising, political campaigning, or political lobbying;

    d. to transmit any material that violates federal, state or local laws;

    e. to engage in "spamming" (sending irrelevant or inappropriate electronic communications individually or en masse) or participate in electronic chain letters;

    f. to violate the "fair use" provisions of the United States Copyright Act of 1976. "Fair use" in this context means that the copyrighted materials of others may be used only for scholarly purposes, and that the use must be limited to brief excerpts;

    g. for bullying, hate mail, defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, gender identity, sexual orientation or disability;

    h. to express vulgar, derogatory, or obscene language;

    i. to post anonymous messages, forge e-mail or mislead as to the true source of an e-mail or author of material;

    j. to log on to someone else's account, attempt to access or change another user's files, or permit anyone else to log on to their own accounts;

    k. to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization, infect the network with a virus, or alter or bypass network files, systems, or securities;

    l. to make money illegally;

m. to develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computer system (e.g., create viruses, worms);

n. to intentionally disrupt information network traffic, crash the network and connected systems, or degrade or disrupt equipment or system performance;

o. to download or save extraordinarily large files without the express approval of the network administrator; or

p. to access, create, or transmit material that is obscene or that promotes illegal acts. If a user accidentally accesses this type of information, he or she should immediately notify a teacher, librarian, and/or network administrator.

4. Network security is everyone's responsibility. Users must observe the username and password protocols which are prescribed by the School District, and may not share usernames/passwords with others. Users are strongly advised to use caution about revealing any information on the Internet which would enable others to exploit them or their identities, including last names, home addresses, Social Security numbers, passwords, credit card numbers or financial institution account information, and photographs. Under no circumstances should a user reveal any information about another person without that person's express prior consent. Users must be aware that any information stored on or communicated through the District network may be susceptible to "hacking" by a third party.

   With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, staff must get approval from the director of technology before authorizing or directing students to use any cloud-based educational software/application. The director of technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements.

5. The District requires that all individual staff/student electronic communications will occur in a manner that will enable the District to independently review all such communication after the fact if the District deems it necessary and appropriate. E-mail using Byram Hills e-mail addresses is the required method of communication between adults and students. It is inappropriate to use electronic communication with a student regarding a matter that does not pertain to school-related activities. Appropriate discussions would include the student's homework, class activity, school sport or club, or other school-sponsored activity. Electronic communications with students are to be sent simultaneously to multiple recipients, not to just one student, except where the communication is clearly school-related and inappropriate for

persons other than the individual student to receive (for example, e-mailing a message about a student's grades). In the event it is not feasible to use e-mail, texts to students must be simultaneously copied to the District cell phone number so it can be documented.

6. Users may wish to create, with approval from the building principal, web content or applications intended to communicate class and school-related information. Websites must reflect the professional image of Byram Hills Central School District, its employees, and students. All subject matter must relate to the schools or the District and must be pertinent to curriculum, instruction, assessment, school-authorized activities, or general information on school operations, and must adhere to Student Privacy Policy 5550. The District assumes no responsibility for student, faculty or staff websites created and/or hosted outside of the District network.

.

Personal Devices: Privacy Considerations

Users are responsible for securing their own electronic devices. The District assumes no responsibility whatsoever for stolen, lost or damaged personal electronic devices or for lost or corrupted data on those devices. This includes devices which are left with a District staff member, whether for the users' convenience or because it has been confiscated for improper use. The District is not responsible for any fees or charges to a user's account. The District technology staff is not responsible for maintaining or troubleshooting a user's personal device. The District is aware that not every student may have access to the same level of personal technology, and will make every reasonable effort to ensure that no student is disadvantaged by permitting the use of personal devices. The use of student-owned devices is optional.

Except as specifically set forth in this policy, no person present on District premises shall make, publish or distribute any photograph, video recording or audio recording (collectively, "Recordings") capturing the image or voice of any other person on District premises (a "Recording Subject") without the express prior permission of the Recording Subject.

The following Recordings may be made <u>without</u> the prior consent of a Recording Subject, subject to any further privacy protections provided by applicable laws and regulations, and provided, further, that no otherwise-permitted Recording shall be distributed or disseminated for the purpose of annoying, embarrassing, intimidating or harassing any Recording Subject:

a. recordings made by or on behalf of authorized District personnel for inclusion in District publications and newsletters, or for dissemination to the news media for the purpose of publicizing District programs or events;

b. recordings made by representatives of news media, parents and other persons lawfully on District premises to attend District events open to visitors, including dramatic productions, athletic events, meetings of the Board of Education and other meetings open to the public on District premises; *provided, however*, that Recordings may be limited in the case of performances of copyrighted material;

c. recordings made in connection with certification and other credentialing processes applicable to teachers and teaching assistants;

d. recordings made with the approval of the Superintendent of Schools for the purpose of assessing or improving the quality of instruction;

e. recordings made by faculty members for educational purposes, or for dissemination only in the faculty member's classroom or school;

f. recordings made by authorized District personnel for use in connection with class photographs, student publications and yearbooks;

g. recordings made and maintained by the District for security purposes;

h. recordings of interior or exterior scenes where the presence of Recording Subjects who have not given consent is merely part of an incidental background; and

i. such other Recordings as are approved in advance by the Superintendent of Schools, an Assistant Superintendent of Schools or a Building Principal, of which approval may include appropriate restrictions.

The District reserves the right to collect and examine any personal or District-owned device for investigation where reasonable suspicion exists that the device is implicated in a violation of this policy or that the integrity of the District's system may have been compromised. Electronic devices are subject to search by school administrators, and the user will be required to unlock the device at the request of the school administrator. Failure to adhere to the aforementioned policies may result in a loss of privilege, confiscation of the device or other disciplinary action, as appropriate.

In addition to other disciplinary, civil or criminal consequences, the District reserves the right to restrict or terminate information network access at any time for any reason.

The Superintendent shall make the final determination as to what constitutes unacceptable use under this policy subject to appeal to the Board of Education. Findings of fact and disciplinary penalties will be determined in accordance with the District's Code of Conduct, and state and federal law. In addition, the District may seek monetary compensation for damages, as appropriate.

Cross Ref:

4526.1 Internet Safety
5300 Code of Conduct
5550 Student Privacy
0115 Student Harassment and Bullying Prevention and Intervention
Parent Bill of Rights

Revised and ADOPTED: 5-9-17